

SHRegGetPath

The destination string buffer must be long enough to hold the return file path.

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4044 bytes

Attack Category	<ul style="list-style-type: none">• Malicious Input• Path spoofing or confusion problem		
Vulnerability Category	<ul style="list-style-type: none">• Buffer Overflow• Unconditional		
Software Context	<ul style="list-style-type: none">• File Path Management		
Location	<ul style="list-style-type: none">• shlwapi.h		
Description	<p>The destination string buffer for SHRegGetPath() must be long enough to hold the return file path. Otherwise, buffer overflows will occur.</p> <p>SHRegGetPath() retrieves a file path from the registry, expanding environment variables as needed.</p>		
APIs	FunctionName	Comments	
	SHRegGetPath		
	SHRegGetPathA	ASCII implementation	
	SHRegGetPathW	Unicode implementation	
Method of Attack	Buffer Overflow		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Whenever SHRegGetPath() is called.	The fourth parameter, pszPath, must be at least MAX_PATH characters in length.	Effective.
Signature Details	DWORD SHRegGetPath(HKEY hkey, LPCTSTR pszSubkey, LPCTSTR pszValue, LPTSTR pszPath, DWORD dwFlags		

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

);	
Examples of Incorrect Code	<pre> TCHAR pszPath[15]; // Buffer is too small HKEY hkey; [...] // set hkey to a handle to a key that is currently open, or a registry root key. DWORD result = SHRegGetPath(hkey, TEXT("MySubKey"), TEXT("MYValue"), pszPath, 0); if (result != ERROR_SUCCESS) { /* handle error */ }</pre>	
Examples of Corrected Code	<pre> TCHAR pszPath[MAX_PATH]; // Buffer is properly sized HKEY hkey; [...] // set hkey to a handle to a key that is currently open, or a registry root key. DWORD result = SHRegGetPath(hkey, TEXT("MySubKey"), TEXT("MYValue"), pszPath, 0); if (result != ERROR_SUCCESS) { /* handle error */ }</pre>	
Source Reference		
Recommended Resources	<ul style="list-style-type: none"> • MSDN reference for SHRegGetPath² • MSDN reference for Registry Functions³ 	
Discriminant Set	Operating System	<ul style="list-style-type: none"> • Windows
	Languages	<ul style="list-style-type: none"> • C • C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>